On 2-level secret sharing schemes (Logics, Algebras and Languages in Computer Science)

AUTHOR(S):

足立, 智子

CITATION:

足立, 智子. On 2-level secret sharing schemes (Logics, Algebras and Languages in Computer Science). 数理解析研究所講究録 2014, 1915: 118-123: KJ00009499499.

ISSUE DATE:

2014-09

URL:

http://hdl.handle.net/2433/223299

数理解析研究所講究録
第1915巻 2014年 118-123

On 2-level secret sharing schemes

Tomoko Adachi
Department of Information Sciences, Toho University,
Miyama 2-2-1, Funabashi, Chiba 274-8510, Japan
E-mail: adachi@is.sci.toho-u.ac.jp

keywords. secret sharing scheme, finite geometry.

Abstract. 2-level shared secret schemes are defined by Simmons in 1989. In this paper, we describe a survey of 2-level secret sharing schemes using finite geometry.

1. Introduction

A secret sharing scheme was introduced by Shamir in 1979 [10] and Blakley in 1979 [4] independently. A secret sharing scheme has been studied by many scientists until today. Now, a secret sharing scheme has some important application to several areas of the information security. In Japan, NRI (Nomura Research Institute) Secure Technologies which is one of the private sector in the area of the information security, has provided clients with some cloud computing product named Secure Cube, from October in 2010. This cloud computing product is utilized by a secret sharing scheme, and is one good example of the application to an external storage unit.

In the situation where the control of an action is shared, the action is only intiated when a predesignated concurrence of participants is obtained. It is a desirable requirement in such a scheme that any grouping of participants other than one of the designated concurrences should have no greater probability of being able to initiate the action than an outsider. Such a scheme is called perfect. Usually the presence of a quorum or threshold of some members of the authorized users is necessary. The question is how to share the secret according to the designated concurrences. In 1989, Simmons [8] defined 2-level shared secret schemes. A

survey of applications of geometric structures in cryptography can be found in a paper of Beutelspacher [1] in 1990. In 1993, Beutelspacher and Wettl [2] study a certain class of 2-level shared secret schemes, using recent results in finite geometry. In 2012, motivated by applications to 2-level secret sharing schemes, Korchmaros, Lanzone and Sonnino [7] investigated k-arcs contained in a $(q+1)$-arc Γ of $PG(3,q)$, q even, which have only a small number of focuses on a real axis of Γ. Doing so, Korchmaros et. al. also investigated hyperfocused and sharply focused arcs contained in a translation oval of $PG(2,q)$.

In this paper, we describe a survey of 2-level secret sharing schemes using finite geometry.

2. 2-level secret sharing schemes using finite geometry

In this section, we describe 2-level secret sharing schemes using finite geometry. At first, we describe secret sharing schemes using finite geometry. Secondly, we describe 2-level secret sharing schemes. Finally, we describe 2-level secret sharing schemes using finite geometry in the case $n+1=3$.

An (n,q)-threshold scheme consist of $k \geq n$ pieces of information, which is called shadows, such that a secret datum can be retrieved from any n or more shadows, but cannot be determined form any $n-1$ or less shadows. We describe a finite geometrical realization of this scheme. Let us define the secret as a point X of a given line s in the projective space $PG(n,q)$, and choose an $(n-1)$-dimensional subspace B, which intersects the line s in X. The line s is known to everybody. Furthermore, we choose as shadows k points P_1, P_2, P_2, $\cdots$, P_k of B, such that the points in the set $\{X, P_1, P_2, P_3, \cdots, P_k\}$ are in general position, that is, any n points of these points generate B.

Next, we describe 2-level secret sharing schemes. Suppose that the set of shadows is divided into two parts $\mathcal{S}$ and $\mathcal{T}$ satisfying the following requirements:

(1) The secret can be reconstructed by any two shaows in $\mathcal{T}$.

(2) The secret can be reconstructed by any $n+1$ shaows in $\mathcal{S} \cup \mathcal{T}$, $(n \geq 2)$.

The secret is shared among a group of participants, which are on two levels. From the top level, one needs just two participants to reconstruct the secret. On the other hand, from the lower level, n participants are

needed to reconstruct the secret. Moreover, it must also be possible to reconstruct the secret if $n-1$ participants of lower level are joined by one top level representative.

Simmons has presented a construction in the case $n+1=3$. (See Simmons [8] and [9].) Suppose the secret is the point X on a given line s in $PG(3,q)$, the set of shadows for the participants on the top level is a subset $\{P_1, P_2, \cdots, P_m\}$ of a line ℓ which intersects s in X, and, the set of shadows for the participants on the lower level is a subset $\mathcal{S}$ of a plane α which intersects s in X and contains ℓ. The set $\{X, P_1, P_2, \cdots, P_m\}$ is denoted by $\mathcal{T}$. Furthermore, $\mathcal{S}$ must be chosen in such a way that no three points of $\mathcal{S}$ are collinear, no two points of $\mathcal{S}$ are collinear with a point of $\mathcal{T}$, and no point of $\mathcal{S}$ is on ℓ. Equivalently, $\mathcal{S}$ must be an arc disjoint from ℓ such that no point of $\mathcal{T}$ is on a secant of $\mathcal{S}$.

3. 2-level secret sharing schemes using finite geometry in the special case $n = 2$

In this section, we describe 2-level secret sharing schemes using finite geometry in the special case $n = 2$.

The construction of Simmons [8], [9] mentioned above led to the next definition.

Definition 2.1 Let $\mathcal{S}$ be a k-arc, and ℓ be a line, no containing any point of $\mathcal{S}$ in finite projective plane. $\mathcal{S}$ is called sharply focused on ℓ, if the secant of $\mathcal{S}$ cover exactly k points of ℓ. $\mathcal{S}$ is called very sharply focused on ℓ, if the secant of $\mathcal{S}$ cover exactly $k-1$ points of ℓ. (See Simmons [9] and Wen-Ai Jackson [6]).

If $\mathcal{S}$ is sharply focused on ℓ and $\mathcal{T}$ is the set of non-covered points of ℓ, then every line through a point of $\mathcal{S}$ has at most one more point of $\mathcal{S} \cup \mathcal{T}$. This observation shows hat results on internal nuclei can be used in the study of sharply focused sets.

Definition 2.2 Let $\mathcal{K}$ be a set of k points of a projective plane π. A point P of $\mathcal{K}$ is called an internal nucleus, if every line hrouge P has at most one more point of $\mathcal{K}$. (See Wettl [12] and [13].)

It follows form this, that the set of nuclei of the set $\mathcal{K} = \mathcal{S} \cup \mathcal{T}$ is $\mathcal{S}$.

The nuclei of k-sets $\mathcal{K}$ in $PG(2,q)$ have been studied by Bichara and Korchmaros [3] for $K = q+2$, by Wettl [12] for $k = q+1$, and by Szony [11] for $k < q+1$. It is clear that the set of nuclei of $\mathcal{S} \cup \mathcal{T}$ is $\mathcal{S}$ if $|\mathcal{T}| \geq 3$.

4. 2-level secret sharing schemes using finite geometry in the general case $n \geq 2$

In this section, we describe 2-level secret sharing schemes using finite geometry in the general case $n \geq 2$.

Let ℓ be a line in the projective space $PG(n,q)$. Let $\mathcal{S}$ and $\mathcal{T}$ be two sets of point in $PG(n,q)$ satisfying the following conditions:

(1) $\mathcal{T}$ is contained in the line ℓ and $|\mathcal{T}| \geq 3$. ($\mathcal{T}$ contains the secret point X.)

(2) $|\mathcal{S}| \geq n+1$.

(3) $\mathcal{S} \cap \mathcal{T} = \emptyset$.

(4) Any subspace generated by n points of $\mathcal{S}$ contains no more points of $\mathcal{S} \cup \mathcal{T}$.

The conditions (2) and (4) together mean that $\mathcal{S}$ is an arc in $PG(n,q)$. We recall that in $PG(n,q)$ a k-arc is a set of k points such as no $m+1$ lie in an $(m-1)$-dimensional space, where $m = 1, 2, \cdots, n$. For $k > n$, this condition holds for all m when it holds for $m = n$. A k-arc $\mathcal{K}$ is called a complete arc, if there is not point P so that $\mathcal{K} \cup \{P\}$ is a $(k+1)$-arc. We observe that if $P_1, P_2, P_3 \in \mathcal{T}$, then $\mathcal{S} \cup \{P_i\}$ is an arc $(i = 1,2,3)$, but $\mathcal{S} \cup \{P_1, P_2, P_3\}$ is not. In other words, $\mathcal{S}$ is a non-complete arc, and there are different complete arcs containing $\mathcal{S}$. Using results on tne lower bound of k for a k-arc having just one completion we get an upper bound of $|\mathcal{S}|$. These results have been proved by Szony [11] for $n = 2$, and by Blokhuis, Bruen and Thas [5] for $n \geq 2$. The generalization of the notion of the internal nuclei to higher dimensions, and another proof of the theorem of Blokhuis, Bruen and Thas [5] can be found in Wettl [13].

References

[1] A. Beutelspacher : Applications of finite geometry to cryptography. *CISM Courses and Lectures*, No. **313** (1990), New York; Springer-Verlag Wien, pp. 161-186.

[2] A. Beutelspacher and F. Wettl : On 2-level secret sharing. *Designs, Codes and Cryptography*, **3** (1993), Kluwer Academic Publishers, pp. 127-134.

[3] A. Bichara and G. Korchmaros : Note on $q+2$-sets in a Galois plane of order q. *Annals of Discrete Math.*, **14** (1982), pp. 117-122

[4] G. R. Blakley : Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, vol. **48** (1979), pp. 313–317.

[5] A. Blokhuis, A. A. Bruen and J. A. Thas : Arcs in $PG(n,q)$, MDS codes and three fundamentalproblems of B. Segre – some extensions. *Geom. Dedicate*, **35** (1990), pp. 1-11

[6] W. A. Jackson : On designs which admit specific automorphisms. Ph. D. Thesis, Royal Holloway and Bedford New College, University of London. (1989).

[7] G. Korchmaros, V. Lanzone and A. Sonnino : Projective k-arcs and 2-level secret sharing schemes. *Designs, Codes and Cryptography*, **64** (2012), Kluwer Academic Publishers, pp. 3-15.

[8] G. L. Simmons : Sharply focused sets of lines on a conic in $PG(2,q)$. *Congressus Numerantium*, **73** (1989), pp. 181-204.

[9] G. L. Simmons : How to (really) share a secret. *Advances in Cryptology – CRYPT '88*, LNCS **403** (1990), pp. 390-448.

[10] Adi Shamir : How to share a secret. *Communications of the ACM*, vol. **22** (1979), pp. 612–613.

[11] T. Szony : k-sets in $PG(2,q)$ having a large set of internal nuclei. *Proc. of "Combinatorics '88* (1991).

[12] F. Wettl : On the nuclei of a pointset of a finite projective plane. *J. of Geometry*, **30** (1987), pp. 157-163.

[13] F. Wettl : Internal nuclei of k-sets in finite projective spaces of three dimensions. *Advances in Finite Geometries and Designs*, (1991), Oxford – New York – Tokyo : Oxford University Press, pp. 407-419.